USAWC STRATEGY RESEARCH PROJECT

INTELLIGENCE: TERRORISM AND HOMELAND DEFENSE

by

COMMANDER JAMES A LOWDER
United States Naval Reserve

Colonel K. L. McClellan
Project Advisor

The views expressed in this academic research paper are those of the author and do not necessarily reflect the official policy or position of the U.S. Government, the Department of Defense, or any of its agencies.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY) 07-04-2003	2. REPORT TYPE	3. DATES COVERED (FROM - TO) xx-xx-2002 to xx-xx-2003

4. TITLE AND SUBTITLE Intelligence: Terrorism and Homeland Defense Unclassified	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Lowder, James A. ; Author	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME AND ADDRESS U.S. Army War College Carlisle Barracks Carlisle, PA17013-5050	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS ,	10. SPONSOR/MONITOR'S ACRONYM(S) 11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE
,

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached file.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 32	19. NAME OF RESPONSIBLE PERSON Rife, Dave RifeD@awc.carlisle.army.mil
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified			19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number DSN

ABSTRACT

AUTHOR: James A. Lowder

TITLE: Intelligence: Terrorism and Homeland Defense

FORMAT: Strategy Research Project

DATE: 07 April 2003 PAGES: 32 CLASSIFICATION: Unclassified

It's said that a good defense is a good offense. To succeed in defending our homeland against terrorist attacks we must take those measures to ascertain, know, and understand the terrorist organizations and the threat they pose. The best instrument in our national power arsenal to do this is the US Intelligence Community (IC) – "our first line of defense." If we are to meet our national strategic objectives to defeat terrorism, to prevent attacks upon our nation and our allies, and to preclude our enemies from threatening us with weapons of mass destruction, then we must effectively collect and analyze intelligence data on the terrorists and then thoroughly disseminate the intelligence products to those organizations best equipped to take the required decisive action against the terrorist groups. This paper will briefly define terrorism, intelligence then review the disciplines of intelligence and the US IC. The types of terrorist organizations will be described followed by some difficulties of the IC leading up to the September 11th attacks on our homeland. General weaknesses of our IC will be discussed followed by some recommendations to strengthen our "first line of defense."

TABLE OF CONTENTS

INTELLIGENCE: TERRORISM AND HOMELAND DEFENSE

> We will direct every resource at our command—every means of diplomacy, every tool of intelligence, every instrument of law enforcement, every financial influence, and every necessary weapon of war—to the disruption and defeat of the global terror network.
>
> —George W. Bush
> September 20, 2001

BACKGROUND AND INTRODUCTION

The September 11, 2001 attacks on the World Trade Center and the Pentagon, preceded by the 1998 bombing of our embassies in Kenya and Tanzania and the 2000 attack against USS Cole, brought the American public to the grisly realization that an international terrorist group, with near impunity, was able to strike us both overseas and in our homeland. There was an ensuing outcry for countermeasures to prevent the possibility of a recurrence and efforts to combat terrorism worldwide had to be undertaken; the underlying element for the effectiveness of these measures remains a strong intelligence program – it is "…the indispensable element of the campaign on which the success of all others will depend."[1]

As Paul R. Pillar, former Director of the Central Intelligence Agency Counterterrorist Center, opined, "The more that intelligence can be relied on as the 'first line of defense' against terrorism . . . the less onerous is the burden on the other defensive lines."[2] Did the United States rely too heavily upon intelligence to provide the first warning of the September 11th attacks and was our first line of defense capable of providing that necessary warning? This paper will review the United States Intelligence Community, centering on its capabilities and shortcomings in combating terrorism, and make recommendations on strengthening our intelligence proficiency.

DEFINITIONS

Terrorism, as defined by the Department of State, is premeditated, politically motivated violence perpetrated against noncombatant targets by sub-national groups or clandestine agents, usually intended to influence an audience.[3]

Domestic terrorism refers to those terrorist activities that occur within the United States proper and perpetrated by US citizens. The 1996 bombing of the federal building in Oklahoma City is an example of domestic terrorism.[4]

International terrorism refers to those terrorist activities that involve the citizens or the territory of more than one country.[5] An example of this type of terrorism is the 2001 terrorist sky-jacking and attacks on the Pentagon and World Trade Center in which citizens from over 90 countries were killed or injured.

A foreign terrorist organization (FTO) is any organization that repeatedly commits acts of violence or threatens violence in pursuit of its political, religious, or ideological objectives. The Secretary of State is empowered to designate FTOs as those groups that conduct international terrorism and threaten our national interests. There are currently 33 terrorists organizations listed as FTOs by the Secretary of State. FTO designation allows the US government to block visas for members of the FTOs without having to prove the individual members were involved in terrorist activities. It also allows our government to block the financial assets of the foreign terrorist organization and any of their designated members, and makes it a criminal act to provide support to the FTO.[6]

State sponsors of terrorism are those countries whose governments have "repeatedly provided support for acts of international terrorism."[7] There are seven nations designated as state sponsors; they are Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria. US law requires the imposition of sanctions against state sponsors of terrorism. The sanctions include restriction on dual use items, prohibition of US official economic assistance, miscellaneous trade restrictions on imports, and a ban on arms exports and sales. Being on this list can also result in sanction laws being applied against persons and countries engaging in certain trade with state sponsors.[8]

Antiterrorism are those actions and defensive measures taken to reduce individual vulnerability and property liability to terrorist acts; antiterrorism includes measures of limited response and containment by military forces.[9]

Counterterrorism are those actions and offensive measures that are taken to prevent, deter, and respond to terrorism.[10]

Combating terrorism are those actions, including antiterrorism and counterterrorism, that are taken to oppose terrorism throughout the entire threat spectrum.[11]

Intelligence is information and knowledge on an adversary or opponent gained through observation, investigation, analysis, and understanding. Intelligence is also the result of collecting, gathering, processing, integrating, analyzing, evaluating, interpreting, and disseminating information concerning foreign countries or areas.[12]

Counterintelligence refers to information gathered and activities conducted to protect our country from espionage, sabotage, assassinations, or other intelligence activities conducted by or for foreign governments, foreign organizations, foreign persons, or international terrorist groups.[13]

Traditionally and in the strictest sense, intelligence is involved only in the collection and analysis of information that is transformed into intelligence with distribution and dissemination limited only to those necessary components or persons requiring the intelligence.[14] Counterintelligence is involved in all related intelligence functions and activities. For the purposes of this paper, intelligence is not solely limited to collecting and analyzing data. Accordingly, this paper will concentrate on the latter description of intelligence.

TYPES OF INTELLIGENCE

There are several types of intelligence, also called intelligence disciplines. They are human intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, open source intelligence, technical intelligence, and finally, counterintelligence.

Human Intelligence is intelligence derived from information collected and provided by humans, more commonly referred to as HUMINT.[15]

Imagery intelligence is intelligence collected from visual photography, infrared sensors, or electro-optics where the images of the objects are reproduced on film or electronically on display devices, also called IMINT.[16]

All source intelligence is intelligence products, organizations, and activities that incorporate all sources of existing information into finished intelligence. It also means in satisfying the intelligence requirements, all collection, exploitation, and processes were identified for possible use and the best and most capable were used.[17]

Open source intelligence is any general, public information that has potential intelligence value.[18]

Scientific and technical intelligence is derived from collecting, interpreting, evaluating, and analyzing foreign scientific and technical developments in applied research and engineering, as well as the scientific and technical capabilities of foreign military systems.[19]

Communications intelligence is technical information intercepted from foreign communications, also called COMINT.[20]

Measurement and signature intelligence is scientific and technical intelligence obtained by the analysis of data derived from sensors for the purposes of identifying distinctive features associated with the targeted sensor, also called MASINT.[21]

Signals intelligence is intelligence derived from foreign communications, electronics, and instruments, also called SIGINT.[22]

Radar intelligence is that intelligence gathered from data collected using radar, also called RADINT.[23]

THE US INTELLIGENCE COMMUNITY

The US Intelligence Community can be grouped into five broad categories. They are national intelligence organizations, Department of Defense (DOD) intelligence organizations, the military service organizations, the unified combatant commanders' intelligence components, and the civilian intelligence organizations. The national intelligence organizations are comprised of the Central Intelligence Agency (CIA), the National Security Agency (NSA), the National Reconnaissance Office (NRO), and the National Imagery and Mapping Agency (NIMA).[24] The Department of Defense (DOD) and military intelligence organizations are comprised of the Defense Intelligence Agency (DIA), the National Military

Joint Intelligence Center (NMJIC), the Army's Intelligence and Security Command (INSCOM) and National Ground Intelligence Center (NGIC), the Navy's Office of Naval Intelligence (ONI) and National Maritime Intelligence Center, the Marine Corps Intelligence Activity, and the US Air Force Directorate of Intelligence, Surveillance, and Reconnaissance (DISR) and Air Intelligence Agency (AIA).[25] The unified and sub-unified combatant commanders rely upon their staff Directorate for Intelligence (J-2) and Joint Intelligence Center (JIC)/Joint Analysis Center (JAC), and the Joint Command and Control Warfare Center (JC2WC) to provide an integrated, coordinated intelligence picture from national and theater sources.[26] The final component of the Intelligence Community is our civilian intelligence organizations. They consist of the Department of State Bureau of Intelligence and Research (INR), the Department of Energy Office of Intelligence (OEI), the Department of Treasury Office of Intelligence Support (OIS), the Department of Commerce Office of Executive Support (OES) and Office of Export Enforcement, the Drug Enforcement Administration (DEA) Intelligence Division, the Federal Bureau of Investigation National Security Division (NSD), and the Department of Transportation Office of Intelligence.[27] Although the interests of these organizations are diverse and different, the underlying goal is the same – to provide finished intelligence products to key decision makers involved in policy, planning, and programming in support of our national strategy, interests and objectives.

INTELLIGENCE IN OUR NATIONAL STRATEGIES

The National Security Strategy for the United States of America forcefully states that the first priority is "to disrupt and destroy terrorist organizations of global reach and attack their leadership; command, control, and communications; material support, and finances."[28] Throughout our National Security Strategy, the President emphasizes that all instruments of our nation's power will be used in combating and ending the terrorist threat against the United States, its allies, and friends. He calls for an "increased emphasis on intelligence collection and analysis"[29] and pledges the necessity to build more integrated intelligence collection capabilities to aid in the early identification of terrorists threats and attacks and "to provide timely, accurate information on threats, wherever they may emerge."[30]

Woven throughout this strategy of making our world safer and better by developing peaceful relations with other nations, increasing political and economic freedom, and enhancing respect for human rights and dignity is the requirement for a more effective intelligence community. The National Security Strategy calls for transforming our intelligence capabilities that had been designed around collecting intelligence on the former Soviet Union into one more suitably integrated into our defense and law enforcement organizations and better coordinated with those same organizations of our allies and friends.

The President outlined several initiatives in the strategy, noting that our intelligence warning and analysis had to be strengthened to ensure an integrated national threat assessment for defense of our homeland and "also ensure the proper fusion of information between intelligence and law enforcement."[31] The initiatives called for strengthening the Director of Central Intelligence authority in leading the actions of our foreign intelligence capabilities; establishing a more seamless and integrated intelligence warning system; developing new methods of collecting information; investing in future capabilities with an increased emphasis on counterintelligence and measures to be taken to preclude any compromise of our intelligence capability; and collecting intelligence about terrorist threats using all source intelligence analysis.[32]

The National Military Strategy of the United States of America clearly states that a safe and secure homeland is the first priority and is fundamental to our military strategy. In order to defend against terrorist attacks on our homeland, our military must possess decision superiority. The strategy asserts that all "decision makers at all levels and echelons require more precise knowledge and decision superiority."[33] We must enhance our ability to collect, analyze, and disseminate "intelligence more effectively in order to function at an operational tempo that adversaries cannot match."[34] This leads to a rapid and robust decision-making. All source intelligence is essential to ensuring our informational and decisional superiority. Timely analysis and rapid dissemination of all source intelligence, as well as effective integration of information systems ensures our military capability to dominate across the full spectrum of conflict.[35]

The National Strategy for Homeland Security defines homeland security as our "concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur."[36] The strategy focuses security functions for homeland defense into six critical areas, two of which are intelligence warning and domestic counterterrorism. The strategy assigns responsibility for counterterrorism to several federal agencies such as the Central Intelligence Agency, the National Institutes of Health, and the Federal Bureau of Investigation. The strategy acknowledges the importance of having timely, disseminated actionable intelligence concerning terrorist activity in the protection of the homeland. Intelligence and information analysis should not be separate, stand alone activities; instead intelligence should be a viable, integral component with four interrelated categories. The categories are:

- tactical threat analysis which allows immediate and near term actions against terrorism to be taken by the appropriate government agency.
- strategic analysis which requires our intelligence organizations to know and understand the roots of international terrorist groups and FTOs, including their current and future capabilities, their financial resources, political support, motivations, and goals.
- vulnerability assessments which allow commanders and planners to project potential consequences of terrorist attacks and take mitigating action to strengthen their defenses.
- threat-vulnerability integration which permits authorities to determine the terrorist organizations posing the greatest threats and the facilities, locales, or sectors most at risk to attack.[37]

This National Strategy claims that intelligence collection and analysis is one of our highest priorities and conveys the idea that the US Intelligence Community should enhance its capability to gather intelligence relevant to homeland security. The strategy calls for us "to do a better job utilizing information contained in foreign-language documents that we have obtained."[38] It also suggests that HUMINT capability and technological advances should be expanded in our intelligence organizations yet only recommends that the FBI's analytical capability be enhanced and that the CIA should loan 25 analysts to the FBI to help improve analytical ability and to boost the FBI/CIA affiliation.[39]

The National Strategy for Combating Terrorism points out that terrorists are using more criminal activities to fund their actions and these groups are sharing intelligence, training areas, logistics, and funding to plan and carry out their attacks. It states that the US Intelligence Community (IC) must continue its aggressive efforts to identify terrorists, their organizations, and support infrastructure. It also notes that the IC should not rely on scientific and technical intelligence but should increase its effort to use other intelligence disciplines, especially HUMINT and linguistic support. The strategy announces the requirement for the IC, along with other federal agencies, to conduct an annual review of internal terrorist sanctuaries and then develop plans to deny terrorist groups access to these areas. The strategy also brings up the importance of "domain awareness" which is the extensive knowledge of events, trends, and activities happening within a specified medium, such as cyberspace. Domain awareness is achieved through the integration and synthesis of all information, data, and intelligence across all agencies. This requires our agencies and forces to have a single integrated operational matrix within their area of responsibility. The document also underscores the Presidential instruction for the Directors of Central Intelligence and FBI, and the Secretaries of Defense and Homeland Security, to establish a Terrorist Threat Integration Center to merge analysis of terrorist intelligence into a single location.[40]

While intelligence is considered our first line of defense against terrorists, collecting it does no good if it is not analyzed and then shared with the other institutions and agencies combating terrorism. Although, legally, the Department of State is the lead agency for countering terrorism outside the United States, logically, the Intelligence Community, headed by the Director of Central Intelligence (DCI), has the lead responsibility in gathering, analyzing, and disseminating intelligence to meet this fundamental layer of defense. In his annual Congressional report, George Tenet, the DCI, acknowledged the importance of the Intelligence Community's capability to provide timely and accurate information to myriad policymakers to prevent attacks.[41]

The Intelligence Community must intensively collect intelligence about the terrorist threat using all sources and has to be integrated with our defense and law enforcement organizations and our allies to be effective.[42] Naturally, the primary point of integration would involve the interagency process and the CIA Counterterrorist Center would be a major player as a proven instrument in interagency cooperation.[43] Presidential Decision Directive 62 (Protection Against Unconventional Threats) further strengthened the interagency cooperation process for intelligence by establishing a National Coordinator for Security, Infrastructure Protection, and Counterterrorism with two senior directors (one for counterterrorism and one for infrastructure protection). It also established a new interagency working group focusing on domestic Weapons of Mass Destruction preparedness.[44] In his annual report to Congress, Director Tenet stated that the DCI's Counterterrorism Center was working with other intelligence offices and the Joint Terrorism Task Force to coordinate intelligence flow to address threats and to facilitate overseas operations to support the war on terrorism so as to "take the war off of US soil."[45] One critical mission area for homeland security is an intelligence system capable of detecting terrorist activity before it develops into an attack.[46] Thus, as stated in our National Strategies, the IC role in counterterrorism relating to homeland defense is to provide the best possible finished intelligence to policymakers so as to prevent terrorist attacks on American territory.

Al Qaeda, Cyber-Terrorism, and Centers of Gravity

There are some general characteristics demonstrated throughout all types of terrorist groups. First, terrorists are insurgents, rebelling against a government or against civil authorities.[47] This rebellion may comprise relatively few members or be a world-side movement. Second, terrorist organizations have an element of ethno-nationalism. They wage conventional and guerrilla warfare against those whose beliefs are different from their own. Recently, terrorism has expanded beyond the confines of single nations or regions and into the international realm. Sabotage combined with international terrorism means that low output from terrorists combined with high damage allows terrorist groups to attain their objectives with little effort.[48]

Terrorist organizations operate over three levels. The lowest level is composed of those terrorist groups that operate within a state or country. The next level, called regional terrorists, involve those terrorist groups that are able to expand their terrorism outside the state boundaries, crossing at least one geographical border. The highest level of terrorist organizations and the ones creating the gravest danger for us and the most difficult to counter, are the global terrorists. These terrorist organizations are able to conduct their activities across several regions and virtually throughout the world. Foreign terrorist organizations that operate internationally pose the greatest threat to our nation, citizens, and national interests.[49]

Although state terrorists can and have inflicted havoc on some of our national interests and serious injury on some of our citizens, they generally are best handled by the intelligence and law enforcement agencies of the countries in which they are operating. Regional terrorist groups usually focus their activities within a specified region; however, they can be supportive to both state and global terrorists. Due to this interconnectivity with global terrorist organizations, regional terrorists are becoming more of a concern for the international community. These groups will require the attention of our instruments of national power to defeat and similar actions taken to counter global terrorists will be necessary against the regional terrorist groups.[50] Of the 33 designated FTOs, 13 are state terrorists groups, 14 operate regionally, and six terrorist organizations can be labeled global terrorists. These are Abu Nidal Organization (ANO), Al-Gama'a al-Islamiyya (Islamic Group), Hizballah (Party of God), Al-Jihad (Egyptian Islamic Jihad), Mujahedin-e Khalq Organization (MEK), and Al Qaeda.[51]

Of these six FTOs, Al Qaeda has caused the most destruction to American interests and citizens over the last nine years. Al Qaeda, meaning 'The Base', was founded by Osama bin Laden, a member of the billionaire Saudi Arabian family that owns the bin Laden Construction Group, in the early 1980's to fight against the Soviet Union's occupation of Afghanistan. Directly beneath bin Laden's leadership is Al Qaeda's Majlis al-Shura which is a consultative council of leaders overseeing the organization's four working committees: military, finance, religious-legal, and the media. Al Qaeda's membership is estimated to be between 3,000 to 5,000 members. Compartmentation and secrecy are paramount within Al Qaeda to ensure its operational efficiency and effectiveness at all levels are maintained.[52]

Osama bin Laden has reportedly inherited millions of dollars that he has used to help finance Al Qaeda's terrorist activities.[53] With the collapse of the Soviet Union, the goal of Al Qaeda changed from expelling Soviet troops from Afghanistan to establishing "a pan-Islamic Caliphate throughout the world by working with allied Islamic extremists groups to overthrow regimes it deems "non-Islamic" and expelling Westerners and non-Muslims from Muslim countries."[54] To demonstrate his pan-Islamic views, and probably to further strengthen Al Qaeda's ties to Muslims world-wide, bin Laden issued a fatwah in February 1998 declaring:

> "To kill Americans and their allies, both civil and military, is an individual duty of every Muslim who is able, in any country where this is possible until the Aqsa Mosque in Jerusalem and the Haram Mosque in Mecca are freed from their grip and until their armies, shattered and broken winged depart from all the lands of Islam and are incapable of threatening any Muslim. . . . By God's leave we call on every Muslin who believes in God and hopes for reward to obey God's command to kill the Americans and plunder their possessions where he finds them and whenever he can."[55]

Al Qaeda has developed associations and ties with other global terrorist organizations such as the Egyptian Islamic Jihad, Hizballah, and the Islamic Group. Al Qaeda has also formed alliances with several state and regional terrorist groups in Sudan, Eritrea, the Philippines, Indonesia, Yemen, Djibouti, Pakistan, and Iran.[56] The purpose of these associations is to provide mutual aid and support in achieving their terrorist objectives. This support can be in the form of financial support, public opinion or media manipulation, or the sharing of personnel, intelligence, safe havens, and/or materials.[57]

Al Qaeda has adeptly used open and available sources, such as cellular telephones and the internet, to communicate with members of its organization and other global FTOs. Information developed and received after September 11th indicates that this FTO had used the internet to organize and plan much of its attacks. Apparently, Al Qaeda operatives in the United States were gathering information and sending it via coded messages over the internet and they continued to do so even after the September 11th attacks. Cyber-planning and cyber-terrorism involve the planning, communication, coordination and actions across the internet that allow for or have an end result of terrorism. There are myriad internet websites that are connected to Al Qaeda that look as if they may be involved in their terrorist planning. By searching the internet, terrorists can find sympathetic and sometimes unknowing helpers for their cause. Listed below are some features of internet technology that must be considered in cyber-terrorism:

- The internet cannot be controlled as can a newspaper through filtering or censorship;
- The internet can be used to recruit new believers and for fundraising without identifying the true organization and its users;
- The internet can be used to plan together or coordinate attacks without identifying the users;

- The internet can be used to gain access to information about targets and to sites that could provide classified information and data;
- The internet can be used to communicate in secret and coded messages;
- The internet can be used to gain access to large amounts of people at once;
- The internet can be used to block business communication and transactions;
- The internet can be used to gather together those of the same thought to invade the cyberspace of others;
- The internet can be used to break the laws of many nations without fear of immediate apprehension;
- And the internet can be used to create diversions from real terrorist events.

We are aware of some of the ways in which Al Qaeda used technology to increase its ability to do significant damage to our homeland. There are now special cyber-operatives in all of our intelligence organizations who are focused on the increased threat of cyber-terrorism.[58]

Our national intelligence agencies and the Defense Intelligence Agency will need to coordinate their efforts in providing the necessary intelligence products to help defeat Al Qaeda. They should focus on the three potential centers of gravity for Al Qaeda – its leadership, financial support, and sanctuaries/safe havens. By maintaining his close allegiances with other terrorist groups and issuing his World Islamic Jihad Fatwah, Osama bin Laden has deepened the support for Al Qaeda throughout the Muslim world and has ensured that his terrorist organization continues to have strategic depth. Accordingly,
to defeat this FTO we will need to concentrate on tracking and eliminating bin Laden from his leadership position. Another strike must be directed at the financial support for Al Qaeda. Its most important funding sources are solicited donations from wealthy individuals, charitable contributions some from legitimate charities unknowingly participating, and black market activity such as drugs, diamond smuggling, and arms trading. It will take a concerted effort by all our intelligence agencies to sort through, analyze, and disseminate the massive amount of information on the financial dealings of Al Qaeda. State sanctuaries and safe havens are another very important center of gravity. No different than other FTOs, Al Qaeda must have safe areas from which to plan its terrorism, train its terrorist operatives, and practice its operations. Failed or failing states and those countries suffering from extreme political instability and weakened economies are the preferred safe havens for the FTOs. We must bring all our national instruments of power to bear on eliminating sanctuaries for the FTOs. Our intelligence

organizations should prove very capable in providing the required intelligence to support this objective.[59]

INTELLIGENCE DIFFICULTIES CONTRIBUTING TO SEPTEMBER 11TH

Bill Gertz, Washington Times reporter, notes, "by far the most damaging intelligence failure was the September 11 terrorist strikes on the World Trade Center and the Pentagon. The attacks succeeded despite the most formidable intelligence-gathering system in the world."[60] Well before the September 11th attacks, the CIA was contacted by but failed to assist some Afghani patriots who were fighting the Taliban, resulting in the execution of some Anti-Taliban warriors. The perceived failure to respond to the many warnings in advance of the attacks is one of the greatest difficulties that our intelligence agencies will have to overcome.[61] For example, when Deputy Director Tenet of the CIA was first informed that a plane has been flown into the World Trade Center, he said to his friend and mentor, David Boren, former retired Chair for the Senate Select Committee on Intelligence: "This is bin Laden. His fingerprints are all over it."[62] Tenet later denied that the bombing of the World Trade Center was a failure of the CIA.[63]

As early as 1995, the US Intelligence Community was aware of Osama bin Laden and his desire to oust Americans from predominantly Muslim countries when Al Qaeda blew up a building in Riyadh, Saudi Arabia, housing the US Army training program for military leaders of Saudi Arabia, killing five Americans and two Saudis.[64]

This was the first terrorist action ordered by and attributed to bin Laden, and started a series of similar attacks often killing not only Americans but also innocent Muslims. Although considered to have the most sophisticated intelligence tracking system in the world, the US was not able to effectively track and monitor bin Laden even though intelligence agencies were aware that he was personally committed to annihilating the US and its holdings. The CIA was aware that he was conducting meetings with officials of countries not friendly to the US and that he was using family money to buy shipments of arms and ammunition.[65]

In 1996, the CIA began earnest effort to track bin Laden and formed a unit to consider the immense amount of information that was being filtered to the agency regarding bin Laden.

Most of the information coming in pointed to his funding terrorism as opposed to his being directly involved.[66] In 1998 allegations regarding bin Laden were so frequent that "President Clinton issued a secret executive order known as a finding that authorized covert action operations against bin Laden."[67]

The State Department Bureau of Intelligence and Research (INR), the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), the Defense Intelligence Agency (DIA) and the National Security Agency (NSA) collected information on bin Laden and concluded that his involvement in terrorist activity against the US could not be determined. In August 1998 car bombs devastated the American embassies in Kenya and Tanzania, killing 220 people and wounding many others; the FBI was aware that Al-Qaeda was responsible. All the above intelligence agencies had received intelligence information that the organization of bin Laden would strike and all had discounted it. Each of the agencies completed appraisals and self-checks and each determined that their agencies were not at fault. Additionally, the political climate and organization of President Clinton may not have supported full accountability of these intelligence organizations. Clinton chose to have bin Laden indicted by a grand jury charging him with conspiracy to kill Americans abroad after bin Laden's Fatwah. Tracking terrorists and their sympathizers clearly justified an increase in intelligence and counterterrorism spending in order to buy the latest technology, fund new operators, and procure new vehicles; however, the extra expenditure of dollars did little to divert the most damaging terrorist attack in America's history.[68]

Often one of our intelligence organizations gathered information on Al Qaeda and another obtained additional information; however, because the agencies did not share information, valuable time was lost in determining what Al Qaeda was going to attempt next. One reason that all of the agencies found it difficult to share information was that Attorney General Janet Reno had, in 1994, established guidelines that prohibited exchange of information from the FBI or CIA to the Internal Security Section of the Justice Department. Basically, it was a question of territoriality because the head of the Justice Department's Office of Policy Review desired to know and be in charge of all that the FBI was collecting in intelligence, specifically in the areas of using electronic intercepts to look for foreign spies who would harm the United States. Many members of the FBI and CIA felt that the rules imposed by Reno inhibited their ability to successfully follow through on information about terrorists.[69]

An example of this could be the case involving Zacarias Moussaoui who was a student at the Pan Am Flight Academy in Minnesota. One of the school's employees contacted the FBI on August 15, 2001 with concerns and worries regarding Moussaoui who had learned to fly small engine planes and now wanted to move onto to Boeing 747 planes. Moussaoui aroused suspicions because he:

- provided little to no information about his previous life;
- paid for his flight training costs of $8,000 in cash, a large amount of money for his apparent means;
- was very interested that the doors of a 747 remain locked during flights;
- only wanted to learn how to bring a plane down and how to take it up;
- was very interested in a flight simulator that took off from Heathrow and landed at Kennedy in New York.

When FBI agents and Immigration officials went to talk to Moussaoui, he became defensive and claimed that he had a student visa and said they were harassing him. The FBI agents wanted to get a warrant to take Moussaoui's computer but were denied because higher headquarters said there was insufficient evidence to show probable cause. The Minneapolis FBI agents contacted the CIA to see if they had any intelligence information about Moussaoui and were met with anger from FBI headquarters for having contacted the CIA about such a matter. The FBI agents then stopped any interaction with the CIA about Moussaoui even though the CIA had information that he had been involved in previous terrorist plans. A request for a warrant on Moussaoui was denied because FBI headquarters did not want to take too aggressive an approach.

After September 11th, Moussaoui's computer was obtained and, in fact, did have information regarding plane-operated suicide attacks, flight simulation programs, wind currents, information about planes and information that led to the grounding of all crop dusters in America for a short period. Based on this incident and others like it, the USA Patriot Act was enacted. Under Section 1861 of this legislation, FBI agents may seek an order requiring an individual or business to provide any tangible evidence to the Bureau on those persons suspected of involvement in foreign intelligence and international terrorism. Additionally, under the Patriot Act, the FBI is able to obtain warrants for wiretaps and electronic surveillance faster and easier because the agency does not have to prove probable cause of a criminal activity on the persons being investigated; the agents only have to provide probable cause that the targeted persons are involved in sabotage or are agents of a foreign power.[70]

Another example of intelligence agencies not sharing information occurred in early October 2000. The DIA's Persian Gulf Division Chief was told by Kie Fallis, one of the agency's top specialists on Iran, that Al Qaeda was planning more terrorist actions against the US. Fallis, using a commercially available software program called *Analyst's Notebook* had tracked many members of the organization and knew that another attack was imminent. Fallis felt strongly that American interests were being threatened. Little did he know that at the same time, bin Laden's terrorist network was planning the USS COLE attack in Yemen and would be successful in their attempt. Fallis was angry because he was sure that the terrorists were linked to Iran. He had been warning his superiors at DIA that there would be an attack in the Persian Gulf and his warnings had been dismissed. Fallis resigned on the day of the USS COLE attack. In his letter to the director of the DIA, Fallis cited analytical differences with his supervisors in the Terrorism Analysis Division and noted that all of his warnings about attacks in the gulf area had been downplayed. He was immediately treated as if he had never been a part of the DIA and an attempt was made to disgrace him by the organization that previously had praised his excellent performance. The DIA went on to deny that any information regarding potential terrorism in Yemen was ever brought forth.[71]

> "Fallis's story is one that demonstrates the problems within the Defense Intelligence Agency and other US intelligence agencies. It highlights some difficulties we have in tracking and preventing terrorist attacks and is representative of a problem of weak leadership, mismanagement and imperfect judgment within our intelligence apparatus."[72]

GENERAL WEAKNESSES OF THE US INTELLIGENCE COMMUNITY

The FBI and CIA have to censor information due to the enormous amount of it coming into their agencies. Often that information is provided by qualified informants and is still determined to be of little intelligence value or is not acted upon. As early as 2000, both the FBI and CIA received information relating to the USS COLE bombing and a reportedly spectacular upcoming operation by Al Qaeda. The information was provided by Robert Baer, a decorated former CIA intelligence officer; but, because he was no longer an official operative deemed in good standing with the agency, his information was ignored. The facts regarding the past inability of the FBI and CIA to detect and promptly act upon intelligence anomalies are apparent in the following list of their organizations' intelligence failures:

- Failure to warn of the 1993 World Trade Center bombing;
- Aldrich Ames, CIA officer, was spying for the Russian government and wasn't detected by the CIA until 1994;
- The 1996 bombing of the Khobar Towers;
- CIA could not determine India's nuclear testing in 1998;
- Robert Hanssen, FBI Counterintelligence Officer, was a Russian spy for over twenty years and wasn't detected by the FBI until 2001.[73]

The Clinton administration made some personnel changes to the FBI that were politically correct but by appointing untrained, ill-prepared minorities to high positions in the organization, did little to improve FBI intelligence collecting abilities. The appointment of Douglas Gow to head the FBI Intelligence Division can be viewed as a serious limitation because Gow had no intelligence background. This appointment and the appointment of others who were not familiar with intelligence caused weaknesses to develop within the agency and may have helped instill a law enforcement approach to intelligence gathering, limiting the ability of the intelligence apparatus of this agency to be successful. Intelligence collection was not a priority at the FBI during the Clinton administration. Instead, the FBI's primary focus was on stopping crime. Funds that had been allocated for intelligence collection were diverted to help with criminal investigation activities. In a climate where terrorists were focusing on the United States and its citizens, the FBI chose to reduce its capability to seek out information that would lead to arrest of individuals who were planning and intent on conducting terrorism.[74]

James J. Angelton, a former CIA Chief of Counterintelligence, opined, "the essence of intelligence work is having the capability to read a foreign target's communications, without the target knowing it."[75] Not believing things to be that simple, Congress became more involved in oversight of our intelligence agencies and may have impacted our IC community's ability to be more effective. By 2001, congressional oversight of intelligence had two results. First, the intelligence services were burdened with a combination of restrictions, constraints and funding controls from the Church and Pike oversight committees. Second, because intelligence agencies had to focus more on Congressional inquiries and testimonies, the community was spending more time and funds on that rather than on improving our intelligence efforts. The intensity of Congressional oversight and the increased number of lawyers being hired at some of the intelligence organizations may have combined to diminish our ability to intercept, read, analyze, and understand the intentions of foreign targets. Our organizations are very good at identifying possible terrorists groups and providing extensive intelligence on them; however, we do not do well at identifying their intentions and preventing their activities.[76]

CONCLUSIONS AND RECOMMENDATIONS

In the aftermath of the September 11th attacks, it is important that our IC learns from past mistakes. In April 2002, Vice President Cheney said,

> ”I don’t, in principal, have any quarrel with the notion of a careful, analytical, and balanced look at how the intelligence community performed prior to 9/11. I would emphasize, I guess, that I think we need to avoid recriminations and a witch-hunt here. The fact of the matter is we’re in the midst of a major conflict, in terms of the war on terrorism. And our intelligence agencies, both foreign and domestic have a major role to play in defending us against further attacks and in helping us prosecute the war.”[77]

He went on to suggest a need to focus on productive changes, working together with all agencies to develop a serious plan for fighting terrorism. In order to develop this serious plan, we need to take a critical look at where we are and what is needed to correct some of our intelligence weaknesses. We need to increase our attention in the areas of improving our intelligence information sharing, enhancing our HUMINT and linguistic capabilities, and updating our national intelligence threat assessment.

Our major endeavors in intelligence now need to be attuned to the ensuing requirements for the newly established Department of Homeland Security and how to take information from all of our intelligence agencies and form it into definitive, focused intelligence products that will enable decision makers to develop plans and actions to prevent further destruction and death through terrorism.

The President’s direction for the FBI, CIA, DOD, and Department of Homeland Security to establish a Terrorist Threat Integration Center must be quickly carried out by all concerned. The purpose and goal of the center is to analyze and fuse all source information relating to terrorist groups. By maintaining and disseminating information from a current threat database, the threat integration center will also enhance the sharing of intelligence information across agencies. The center will also be responsible for providing terrorist threat assessments to our policy makers.[78] This is a fundamental first step in making certain our intelligence collection products are properly shared by all applicable intelligence organizations to enhance and strengthen our capability to provide for adequate homeland defense.

American intelligence organizations need to actively seek to expand their HUMINT structure and linguistic capability. The Intelligence Community currently relies too much on scientific and technical intelligence. The drawback of this over-reliance is that scientific and technical intelligence collection rarely provides insights into the intentions and plans of terrorists. Human intelligence can provide additional information that could substantiate a correct course of action or negate a potential intelligence slip-up. In the past, the DCI has been reluctant to recruit human intelligence agents from FTOs. Former DCI Deutsch enacted certain rules against recruiting any person who had a past history of violent behavior to ensure that our human intelligence sources could be trusted and possess the right integrity to provide valid, accurate information. Section 903 of the USA Patriot Act (Public Law 107-56) expressed that intelligence officials should be encouraged and make every effort to establish and maintain intelligence relationships with any persons, entity or group to obtain the necessary information on terrorists. The FY02 Intelligence Authorization Act (Public Law 107-108) directs the DCI to relax the restrictions against recruiting human agents in terrorist organizations.[79] The National Commission on Terrorism also notes the importance of aggressively recruiting human intelligence sources, stating that it should be one of IC's priorities.[80] The National Commission on Terrorism recommended the DCI "authorize the Foreign Language Executive Committee to develop a larger pool of linguists and an interagency strategy for employing them."[81] The initiative to improve our HUMINT and linguistic abilities is paramount to ensure we take the appropriate action to resolve intelligence collection inadequacies and weaknesses.

Finally, we need a current terrorist threat baseline assessment. Congressman Christopher Shays, Sub-committee Chair on National Security, called for a formal assessment of domestic and foreign threats "to provide an authoritative, comprehensive and intelligence-based overview. It should be updated regularly and it should be shared . . . to the fullest extent possible."[82] We must ensure our National Intelligence Estimate (NIE) is kept current. As Dr. Bruce Hoffman, Director of Rand's Washington Office, pointed out, "the last comprehensive national intelligence estimate regarding foreign terrorist threats—a prospective, forward-looking effort to predict and anticipate future terrorist trends—was conducted nearly a decade ago."[83] Unless we have thorough ongoing, comprehensive re-assessments of our NIE we cannot be sure that the range of our policies, and our defensive and offensive measures are appropriate and effective in combating terrorism.[84] Without an updated threat assessment we will not have the necessary information and intelligence to ensure we have adopted the best measures to protect our homeland.

Word Count: = 6973.

ENDNOTES

[1] Kurt M. Campbell and Michele A. Flournoy, “Intelligence: The Long Pole in the Tent,” in To Prevail: An American Strategy for the Campaign Against Terrorism (Washington, DC: CSIS Press, 2001), 77.

[2] Paul R. Pillar, “Counterterrorist Instruments,” in Terrorism and U.S. Foreign Policy (Washington, DC: Brookings Institution, 2001), 116.

[3] US Department of State, Patterns of Global Terrorism 2001 (Washington, DC: US Government Printing Office, May 2002), xvi.

[4] Ian O. Lesser et al., Countering the New Terrorism (Washington, DC: Rand, 1999), 86.

[5] US Department of State, Patterns of Global Terrorism 2001, xvi.

[6] Ibid., 87, 144.

[7] Ibid., 144.

[8] Ibid.

[9] US Joint Chiefs of Staff, Joint Tactics, Techniques, and Procedures for Antiterrorism, Joint Publication 3-07.2 (Washington, DC: US Joint Chiefs of Staff, 17 March 1998), GL-3.

[10] Ibid.

[11] Ibid.

[12] US Joint Chiefs of Staff, Doctrine for Intelligence Support to Joint Operations, Joint Publication 2-0 (Washington, DC: US Joint Chiefs of Staff, 9 March 2000), GL-5.

[13] Ibid., GL-3.

[14] Jeffrey T. Richelson, The U.S. Intelligence Community (Boulder, CO: Westview Press, 1999), 3.

[15] US Joint Chiefs of Staff, Doctrine for Intelligence Support to Joint Operations, GL-4.

[16] US Joint Chiefs of Staff, National Intelligence Support to Joint Operations, Joint Publication 2-02 (Washington, DC: US Joint Chiefs of Staff, 28 September 1998), GL-8.

[17] Ibid., GL-6.

[18] Ibid., GL-11.

[19] Ibid., GL-12.

[20] Ibid., GL-6.

[21] Ibid., GL-10.

[22] Ibid., GL-12.

[23] Ibid.

[24] Richelson, 16.

[25] Ibid., 55-103.

[26] US Joint Chiefs of Staff, Doctrine for Intelligence Support to Joint Operations, I-7-I-9, IV-1-IV-7.

[27] Richelson, 130-143.

[28] George W. Bush, The National Security Strategy of the United States of America (Washington, DC: The White House, September 2002), 5.

[29] Ibid., 14.

[30] Ibid., 16.

[31] Ibid., 30.

[32] Ibid.

[33] US Joint Chiefs of Staff, The National Military Strategy of the United States of America (Washington, DC: US Joint Chiefs of Staff, 28 September 2002), iv.

[34] Ibid., 30.

[35] Ibid., 14, 30-31.

[36] George W. Bush, National Strategy for Homeland Security (Washington, DC: The White House, July 2002), 2.

[37] Ibid., 16-17.

[38] Ibid., 16.

[39] Ibid., 17-18.

[40] George W. Bush, National Strategy for Combating Terrorism (Washington, DC: The White House, February 2003), 8, 16, 22, 25-26.

[41] George J. Tenet, Director of Central Intelligence Annual Report of the United States Intelligence Community Fiscal Year 2001 (Washington, DC: U.S. Central Intelligence Agency, 2002), 2.

[42] Bush, The National Security Strategy of the United States of America, 30.

[43] Arthur S. Hulnick, “Interagency Cooperation,” in Fixing the Spy Machine (Westport, CT: Prager, 1999), 198.

[44] Raphael F. Perl, Terrorism, the Future, and U.S. Foreign Policy (Washington, DC: Congressional Research Service, September 2001), 10.

[45] Tenet, 15.

[46] Bush, National Strategy for Homeland Security, viii.

[47] Paul Wilkinson, Terrorism Versus Democracy The Liberal State Response (Portland, OR: Frank Cass Publishers, 2001), 2.

[48] Ibid., 13-18.

[49] National War College, Combating Terrorism in a Globalized World: Report by the National War College Student Task on Combating Terrorism (Washington, DC: National War College, May 2002), 11.

[50] Ibid.

[51] US Department of State, Patterns of Global Terrorism 2001 (Washington, DC: Department of State, May 2002), 87-111.

[52] National War College, 16-17.

[53] US Department of State, 106.

[54] Ibid., 105.

[55] Gertz, Bill, Breakdown How America's Intelligence Failures Led to September 11 (Washington, DC: Regnery Publishing, Inc., 2002), 19.

[56] Ibid., 230-231.

[57] National War College, 10-13.

[58] Timothy L. Thomas, "Al Qaeda and the Internet: The Danger of Cyberplanning," Parameters 33 (Spring 2003): 112-123.

[59] National War College, 17-19.

[60] Gertz, 4.

[61] Ibid., 1-4.

[62] Ibid., 59.

[63] Ibid., 5.

[64] Ibid., 7-8.

[65] Ibid., 7-18.

[66] Ibid., 12.

[67] Ibid., 13.

[68] Ibid., 5-20.

[69] Ibid., 29-30, 33.

[70] Ibid., 20-38, 88.

[71] Ibid., 39-52.

[72] Ibid., 43.

[73] Ibid., 59,62,98.

[74] Ibid., 90-103.

[75] Ibid., 105-106.

[76] Ibid., 105-125.

[77] Ibid., 117.

[78] George W. Bush, Fact Sheet: Strengthening Intelligence to Better Protect America (Washington, DC: The White House, January 23, 2003); available from <http://www.whitehouse.gov/news/releases/2003/01/20030128-12.html>; Internet; accessed 1 April 2003.

[79] Richard A. Best, Jr., Intelligence Issues for Congress, CRS Issue Brief for Congress (Washington, DC: Congressional Research Service, January 8, 2002), CRS-4-CRS-5.

[80] Paul L. Bremer, III, Countering the Changing Threat of International Terrorism, Report from the National Commission

on Terrorism to the 105th Congress (Washington, DC, 2001), 10.

[81] Ibid., 14.

[82] Christopher Shays, Combating Terrorism: In Search ofStrategy, Priorities and Leadership, Speech presented to the National Governors Association Center for Best Practices National Emergency Management Association (Washington, DC: July, 2001), 3.

[83] Bruce Hoffman, Combating Terrorism :In Search of a National Strategy, Testimony Before the Subcommittee on National Security, Veterans Affairs, and International Relations, House Committee on Government Reform (Washington, DC: Rand Corp, March 27, 2001), 3.

[84] Ibid., 7.

BIBLIOGRAPHY

Best, Richard A., Jr. Intelligence Issues for Congress. CRS Issue Brief for Congress. Washington, DC: Congressional Research Service, January 8, 2002.

Bremer, Paul L., III. Countering the Changing Threat of International Terrorism. Report from the National Commission on Terrorism to the 105th Congress. Washington, DC, 2001.

Bush, George W. National Strategy for Homeland Security. Washington, DC: The White House, July 2002.

________. National Strategy for Combating Terrorism. Washington, DC: The White House, February 2003.

________. The National Security Strategy of the United States of America. Washington, DC: The White House, September 2002.

________. Fact Sheet: Strengthening Intelligence to Better Protect America. Washington, DC: The White House, January 23, 2003. Available from <http://www.whitehouse.gov/news/releases/2003/01/20030128-12.html>. Internet. Accessed 1 April 2003.

Campbell, Kurt M., and Michele A. Flournoy. “Intelligence: The Long Pole in the Tent.” In To Prevail: An American Strategy for the Campaign Against Terrorism. Washington, DC: CSIS Press, 2001.

Gertz, Bill. Breakdown How America’s Intelligence Failures Led to September 11. Washington, DC: Regnery Publishing, Inc., 2002.

Hoffman, Bruce. Combating Terrorism:In Search of a National Strategy. Testimony Before the Subcommittee on National Security, Veterans Affairs, and International Relations, House Committee on Government Reform. Washington, DC: Rand Corp, March 27, 2001.

Hulnick, Arthur S. “Interagency Cooperation.” In Fixing the Spy Machine. Westport, CT: Prager, 1999.

Lesser, Ian O., Hoffman, Bruce, Arquilla, John, Ronfeldt, David, and Zanini, Michele. Countering the New Terrorism. Washington, DC: Rand, 1999.

National War College. Combating Terrorism in a Globalized World: Report by the National War College Student Task on Combating Terrorism. Washington, DC: National War College, May 2002.

Perl, Raphael F. Terrorism, the Future, and U.S. Foreign Policy. Washington, DC: Congressional Research Service, September 2001.

Pillar, Paul R. “Counterterrorist Instruments” In Terrorism and U.S. Foreign Policy. Washington, DC: Brookings Institution, 2001.

Richelson, Jeffrey T. The U.S. Intelligence Community. Boulder, CO: Westview Press, 1999.

Shays, Christopher. Combating Terrorism: In Search of Strategy, Priorities and Leadership. Speech presented to the National Governors Association Center for Best Practices National Emergency Management Association. Washington, DC. July, 2001.

Smith, James M., and Thomas, William C., eds. The Terrorism Threat and U.S. Government Response: Operational and Organizational Factors. USAF Academy, CO: USAF Institute For National Security Studies, 2001.

Steele, Robert D. “Key Aspects of Intelligence as a Craft.” In The New Craft of Intelligence: Personal, Public, & Political-Citizen’s Action Handbook for Fighting Terrorism, Genocide, Disease, Toxic Bombs, & Corruption. Oakton, VA: OSS International Press, 2001.

Tenet, George J. Director of Central Intelligence Annual Report of the United States Intelligence Community Fiscal Year 2001. Washington, DC: U.S. Central Intelligence Agency, 2002.

Thomas, Timothy L. “Al Qaeda and the Internet: The Danger of Cyberplanning.” Parameters 33 (Spring 2003): 112-123.

US Department of State. Office of the Coordinator for Counterterrorism. Patterns of Global Terrorism 2001. Washington, DC: Department of State, May 2002.

US Joint Chiefs of Staff. Joint Tactics, Techniques, and Procedures for Antiterrorism. Joint Publication 3-07.2. Washington, DC: US Joint Chiefs of Staff, 17 March 1998.

________. Doctrine for Intelligence Support to Joint Operations. Joint Publication 2-0. Washington, DC: US Joint Chiefs of Staff, 9 March 2000.

________. National Intelligence Support to Joint Operations. Joint Publication 2-02. Washington, DC: US Joint Chiefs of Staff, 28 September 1998.

________. National Military Strategy of the United States of America. Washington, DC: US Joint Chiefs of Staff, 19 September 2002.

Wilkinson, Paul. Terrorism Versus Democracy The Liberal State Response. Portland, OR: Frank Cass Publishers, 2001.